ELLIPTIC CURVE CRYPTOGRAPHY

PRESENTED BY :

MRS. S J PATEL

DEPARTMENT OF COMPUTER ENGINEERING,

NIT, SURAT

Elliptic Curve Cryptography: Motivation

- Public key cryptographic algorithms (asymmetric key algorithms) play an important role in providing security services:
  - Confidentiality
  - Key management
  - User authentication
  - Signature
- Public key cryptography systems are constructed by relying on the hardness of mathematical problems
  - RSA: based on the integer factorization problem
  - DH: based on the discrete logarithm problem
- The main problem of conventional public key cryptography systems is that the key size has to be sufficient large in order to meet the high-level security requirement.
- This results in lower speed and consumption of more bandwidth
  - Solution: Elliptic Curve Cryptography system

Introduction to Elliptic Curves

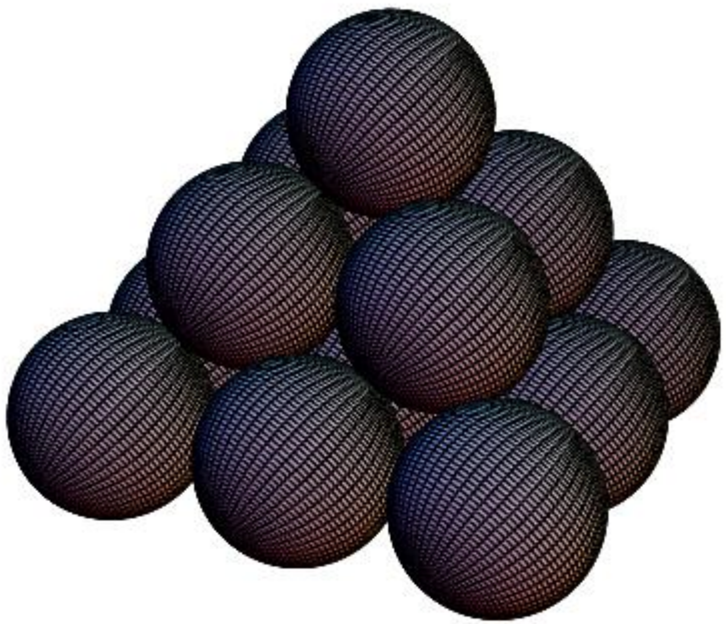
- Lets start with a puzzle…

What is the number of balls that may be piled as a square pyramid and also rearranged into a square array?

Introduction to Elliptic Curves

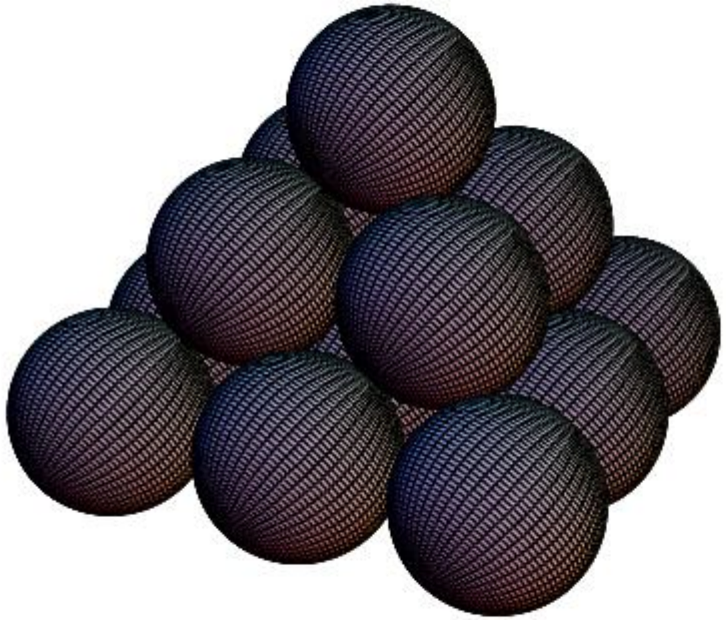
- Lets start with a puzzle…

  What is the number of balls that may be piled as a square pyramid and also rearranged into a square array?



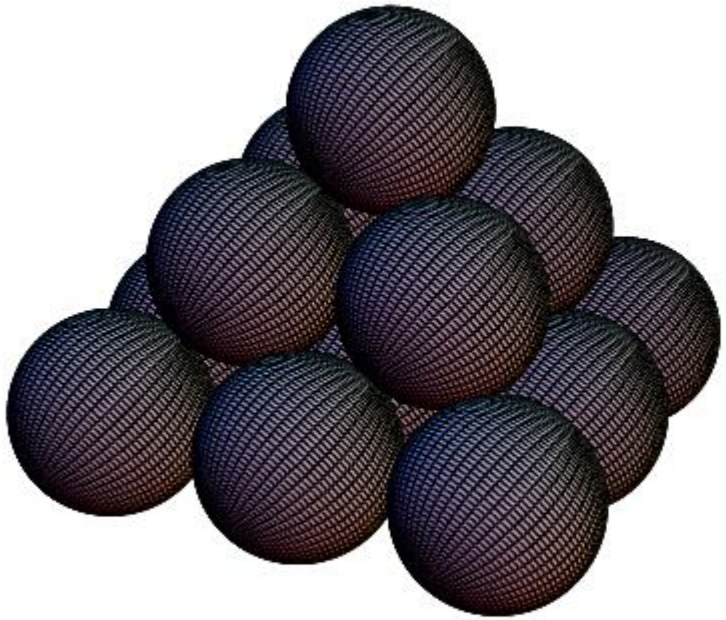
Introduction to Elliptic Curves

- What about the figure shown?
- *Does it fulfil our requirements?*



Introduction to Elliptic Curves

- What about the figure shown?
- *Does it fulfil our requirements???*
- *Can you find solutions to this problem???*



Introduction to Elliptic Curves

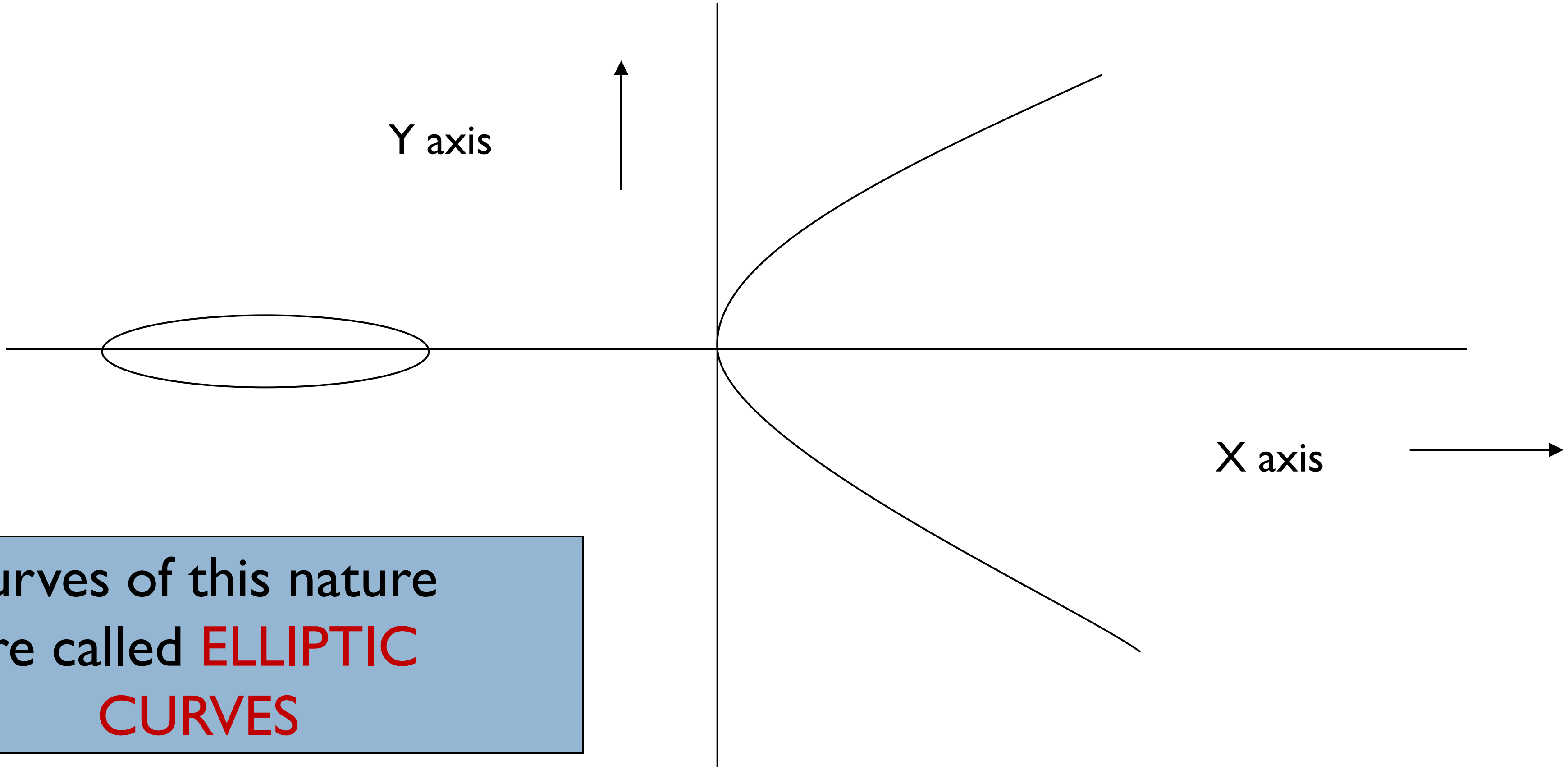
- Let x be the height of the pyramid, then the number of balls in pyramid is,

$$1^2 + 2^2 + 3^2 + \ldots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

- We also want this to be a square. Hence,

$$y^2 = \frac{x(x+1)(2x+1)}{6}$$

Graphical Representation



Curves of this nature are called ELLIPTIC CURVES

Method of Diophantus

- Uses a set of known points to produce new points
- (0,0) and (1,1) are two trivial solutions
- Equation of line through these points is y=x.
- Intersecting with the curve and rearranging terms:

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$$

- What are the roots of this equation???

Method of Diophantus

- Uses a set of known points to produce new points
- (0,0) and (1,1) are two trivial solutions
- Equation of line through these points is y=x.
- Intersecting with the curve and rearranging terms:

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$$

- What are the roots of this equation???
  - Two trivial roots x=0 and x=1…… But what about third one????

Method of Diophantus

- We know that, for any numbers a,b,c, we have,

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+bc+ac)x - abc$$

- Hence, for the equation

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$$

- We have,

$$a+b+x = \frac{3}{2} \rightarrow 0+1+x = \frac{3}{2} \rightarrow x= \frac{1}{2}$$

- Hence, one more point (½ , ½) and because of the symmetry , another (½ , -½)

Method of Diophantus : Exercise

- Can you find out another point on curve using Diophantus's method ???

Consider two points (½ ,-½) and (1,1) and find out another point on the curve …..

Method of Diophantus : Exercise solution

- Consider the line through (1/2,-1/2) and (1,1) => y=3x-2
- Intersecting with the curve we have:

$$x^3 - \frac{51}{2}x^2 + \ldots = 0$$

- Thus ½ + 1 + x = 51/2 or x = 24 and y=70
- Thus if we have 4900 balls we may arrange them in either way

Weierstrass Equation

- For most situations, an elliptic curve E is the graph of an equation of the form:

$$y^2 = x^3 + Ax + B$$

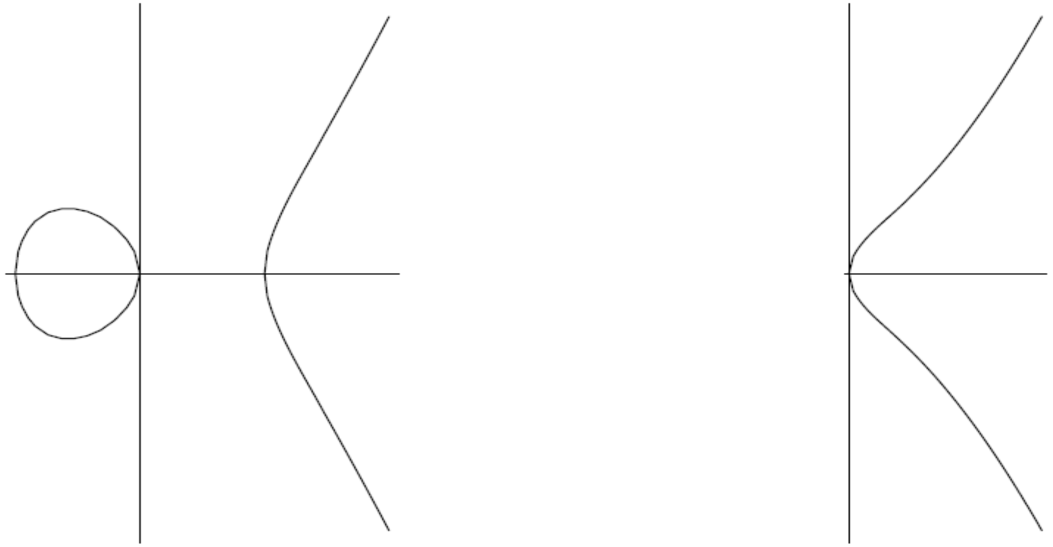
where A and B are constants. This refers to the Weierstrass Equation of Elliptic Curve.

- Here, A, B, x and y all belong to a field of say rational numbers, complex numbers, finite fields (F_p) or Galois Fields ($GF(2^n)$).
- If K is the field where A,B $\in$ K, then we say that the Elliptic Curve E is defined over K

Points on Elliptic Curve

- If we want to consider points with coordinates in some field *L*, we write *E(L)*. By definition, this set always contains the point ∞

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}$$



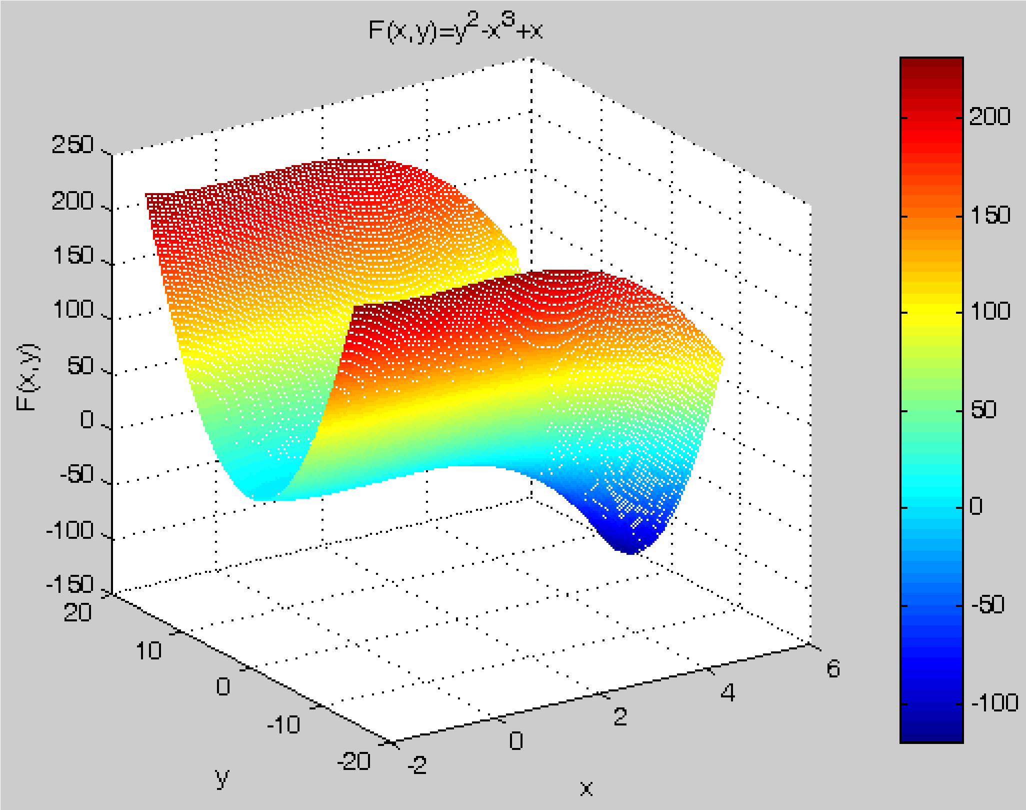
(a) $y^2 = x^3 - x$ (b) $y^2 = x^3 + x$

What about the roots of these curves ????

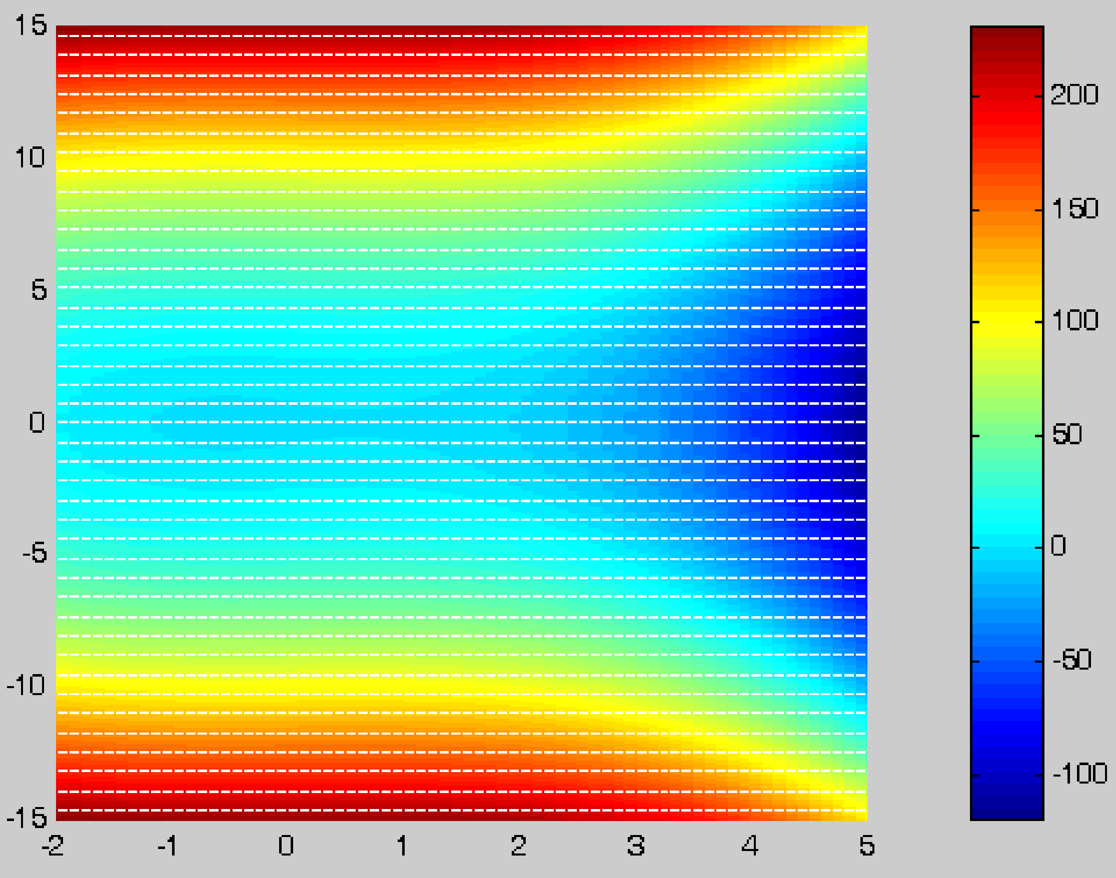
We must have the equation $4A^3 + 27B^2 \neq 0$ satisfied

A condition for an Elliptic curve to be a group !!!!!

Points on Elliptic Curve

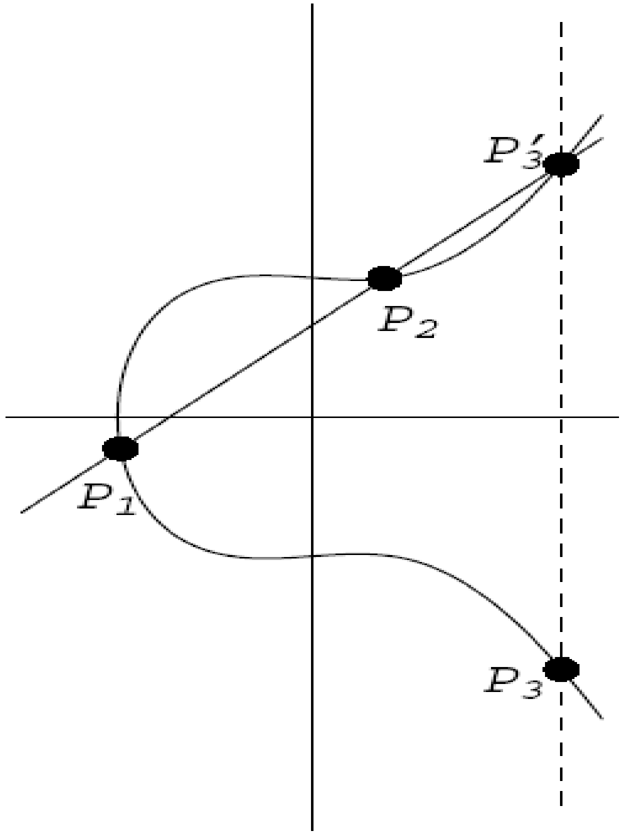


Points on Elliptic Curve



Adding points on Elliptic Curve

- Start with two points : $P_1(x_1,y_1)$ and $P_2(x_2,y_2)$ on elliptic curve
- To get a new point P_3 , $y^2 = x^3 + Ax + B$
  - Draw a line L through P_1 and P_2
  - Get the intersection P_3'
  - Reflect across x-axis to get P_3
- We define $P_1 + P_2 = P_3$



Adding points on Elliptic Curve (cont.)

- Case I: $P_1 \neq P_2$ and neither point is ∞
  - For $x_1 \neq x_2$
  - For $x_1 = x_2$????
    - We get $P_1 + P_2 = \infty$
- Case II : $P_1 = P_2 = (x_1, y_1)$

Slope of the line L passing through P_1 and P_2 is,

$$m = \frac{(y_2 - y_1)}{(x_2 - x_1)}$$

For $x_1 \neq x_2$, equation of line L is,

$$y = m(x - x_1) + y_1$$

To find intersection with E, substitute to get,

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

Rearrange to form,

$$0 = x^3 - m^2 x^2 + \ldots$$

Given two roots x_1 and x_2, third root can be calculated,

$$(a + b + c) = m^2 \Rightarrow (x_1 + x_2 + x) = m^2$$

$$\Rightarrow x = m^2 - x_1 - x_2$$

and $y = m(x - x_1) + y_1$

refecting across the x - axis to obtain the point $P_3 = (x_3, y_3)$:

$$x_3 = m^2 - x_1 - x_2 \text{ and } y_3 = m(x_1 - x_3) - y_1$$

Adding points on Elliptic Curve (cont.)

- Case II : $P_1 = P_2 = (x_1, y_1)$
  - When two points on a curve are very close to each other, the line through them approximates a tangent line. Therefore, when the two points coincide, we take the line *L* through them to be the tangent line.
  - Implicit differentiation allows us to find the slope *m of L*

$$2y\frac{dy}{dx} = 3x^2 + A, \text{so } m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

If $y_1 \neq 0$, the equation of L is,

$$y = m(x - x_1) + y_1$$

We find the cubic equation,

$$0 = x^3 - m^2 x^2 + \dots$$

This time we know only one root x_1, we obtain :

$$x_3 = m^2 - 2x_1, \quad y_3 = \mathrm{m}(x_1 - x_3) - y_1$$

Adding points on Elliptic Curve (cont.)

- Case II : $P_1 = P_2 = (x_1, y_1)$
  - If $y_1 \neq 0$
  - If $y_1 = 0$
    - We get $P_1 + P_2 = \infty$
- Case III: $P_2 = \infty$
  - What about $P_1 + P_2$????
  - Do we get $P_1 + P_2 = P_1$??
  - In other words, $P_1 + \infty = P_1$

Group Law

- The addition of points on an elliptic curve E satisfies the following properties:
  - (Commutativity) : $P_1 + P_2 = P_2 + P_1$ for all P_1, P_2 on E
  - (Existence of identity) : $P + \infty = P$ for all P on E
  - (Existence of inverses) : Given P on E, there exists P' on E with $P + P' = \infty$. This point P' will usually be denoted as –P
  - (Associatively) : $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all P_1, P_2, P_3 on E

The points on E form an additive abelian group with ∞ as the identity element.

Integer times a point

- Let k be a positive integer and let P be a point on an elliptic curve, then
  - kP denotes P + P + · · · + P (with k summands)
- Efficient computation for large k
  - Successive doubling method
    - For example, to compute 19*P, we compute*
      - *2P, 4P = 2P+2P, 8P = 4P+4P, 16P = 8P+8P, 19P = 16P+2P+P.*
- But, the only difficulty is....
  - The size of the coordinates of the points increases very rapidly if we are working over the rational numbers
  - What about finite fields ????

ELLIPTIC CURVES IN CRYPTOGRAPHY

Elliptic curves in Cryptography

- Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.
- The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field.

Why finite field?

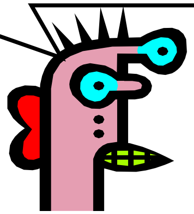
- Elliptic curves over real numbers
  - Calculations prove to be slow
  - Inaccurate due to rounding error
  - Infinite field
- Cryptographic schemes need fast and accurate arithmetic
- In the cryptographic schemes, elliptic curves over two finite fields are mostly used.
  - Prime field F_p , where p is a prime.
  - Binary field F_{2^m}, where m is a positive integer

DISCRETE LOGARITHMS IN FINITE FIELDS

F={1,2,3,…,p-1}

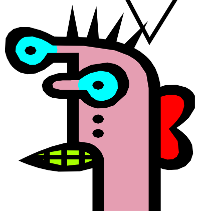
Pick secret, random X from F

Pick secret, random Y from F



g^x mod p →

← g^y mod p



Alice

Bob

Compute $k=(g^y)^x=g^{xy}$ mod p

Compute $k=(g^x)^y=g^{xy}$ mod p

Eve has to compute g^{xy} from g^x and g^y without knowing x and y…
She faces the Discrete Logarithm Problem in finite fields

Elliptic curves over finite fields

- Let us do an exercise....
- Let E be the curve $y^2 = x^3+x+1$ over F_5, find all the points on E

Therefore, $E(F_5)$ has order 9.

Can you show that $E(F_5)$ is cyclic??? What is the generator??

x	x^3+x+1	y	Points
0	1	± 1	(0,1),(0,4)
1	3	-	-
2	1	± 1	(2,1),(2,4)
3	1	± 1	(3,1),(3,4)
4	4	± 2	(4,2),(4,3)
∞		∞	∞

Elliptic curves over finite fields : Exercise

- Let E be the curve $y^2 = x^3+2$ over F_7, find all the points on E

What is the order of $E(F_7)$?

Is $E(F_7)$ cyclic??? If yes, what is the generator??

x	x^3+2	y	Points

Elliptic curves over finite fields : Exercise

- Let E be the curve $y^2 + xy = x^3 + 1$ over F_2, find all the points on E

What is the order of $E(F_2)$?

Is $E(F_2)$ cyclic??? If yes, what is the generator??

x	x^3-xy+1	y	Points

Elliptic curve discrete logarithm problem

If we are working over a large finite field and are given points P and kP, it is computationally hard to determine the value of k. This is called the ***discrete logarithm problem for elliptic curves (ECDLP)*** *and is the basis for the cryptographic applications.*

What Is Elliptic Curve Cryptography (ECC)?

- Elliptic curve cryptography [ECC] is a **public-key** cryptosystem just like RSA, El Gamal.
- Every user has a **public** and a **private** key.
  - Public key is used for encryption/signature verification.
  - Private key is used for decryption/signature generation.
- Elliptic curves are used as an extension to other current cryptosystems.
  - Elliptic Curve El-Gamal Encryption
  - Elliptic Curve Diffie-Hellman Key Exchange
  - Elliptic Curve Digital Signature Algorithm

Using Elliptic Curves In Cryptography

- The central part of any cryptosystem involving elliptic curves is the **elliptic group**.
- All public-key cryptosystems have some underlying mathematical operation.
  - RSA has exponentiation (raising the message or ciphertext to the public or private values)
  - ECC has point multiplication (repeated addition of two points).

Discrete Logarithm Key pair generation

- A key pair is associated with a set of public domain parameters *(p,q, g). Here, p is a prime, q is a prime divisor of p−1, and g ∈ [1, p−1] has order q*

INPUT: DL domain parameters (p,q, g).

OUTPUT: Public key y and private key x.

1. Select $x \in_R [1, q-1]$.

2. Compute $y = g^x \bmod p$

3. Return (y,x).

ECC Key pair generation

- Let E be an elliptic curve defined over a finite field F_p.
- Let P be a point in $E(F_p)$, and suppose that P has prime order n. Then the cyclic subgroup of $E(F_p)$ generated by P is,

$$P = \{\infty, P, 2P, 3P, \ldots, (n-1)P\}.$$

The public domain parameters are : The prime p, the equation of the elliptic curve E, and the point P and its order n : (p,E,P,n)

A private key is an integer d that is selected uniformly at random from the interval $[1, n-1]$, and the corresponding public key is $Q = dP$.

Basic Elgamal encryption scheme

Basic ElGamal Encryption

INPUT: DL domain parameters (p,q,g), public key y, plaintext $m \in [0, p-1]$.

OUTPUT: Ciphertext (c_1, c_2).

1. Select $k \in_R [1, q-1]$.

2. Compute $c_1 = g^k \bmod p$

3. Compute $c_2 = m \cdot y^k \bmod p$

2. Return (c_1, c_2).

Basic ElGamal Decryption

INPUT: DL domain parameters (p,q,g), private key x, ciphertext (c_1, c_2).

OUTPUT: Plaintext m.

1. Compute $m = c_2 \bullet c_1^{-x} \bmod p$.

2. Return (m).

ECC Analog to El Gamal : ECEG

EC-ElGamal Encryption

INPUT: Elliptic curve domain parameters (p, E, P, n), public key Q, plaintext m.
OUTPUT: Ciphertext (C_1, C_2)

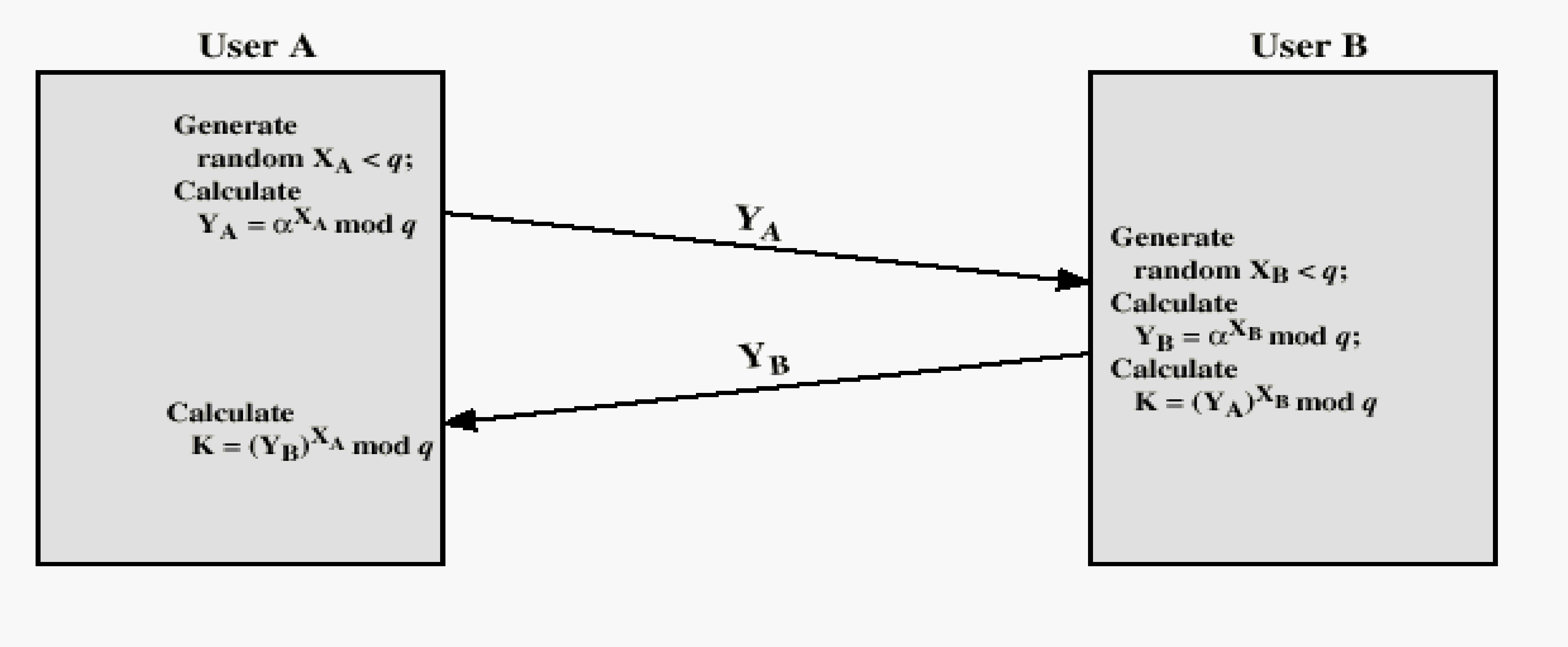
1. Represent the message m as a point M in $E(F_p)$
2. Select $k \in_R [1, n-1]$.
3. Compute $C_1 = kP$.
4. Compute $C_2 = M + kQ$.
5. Return (C_1, C_2).

EC-ElGamal Decryption

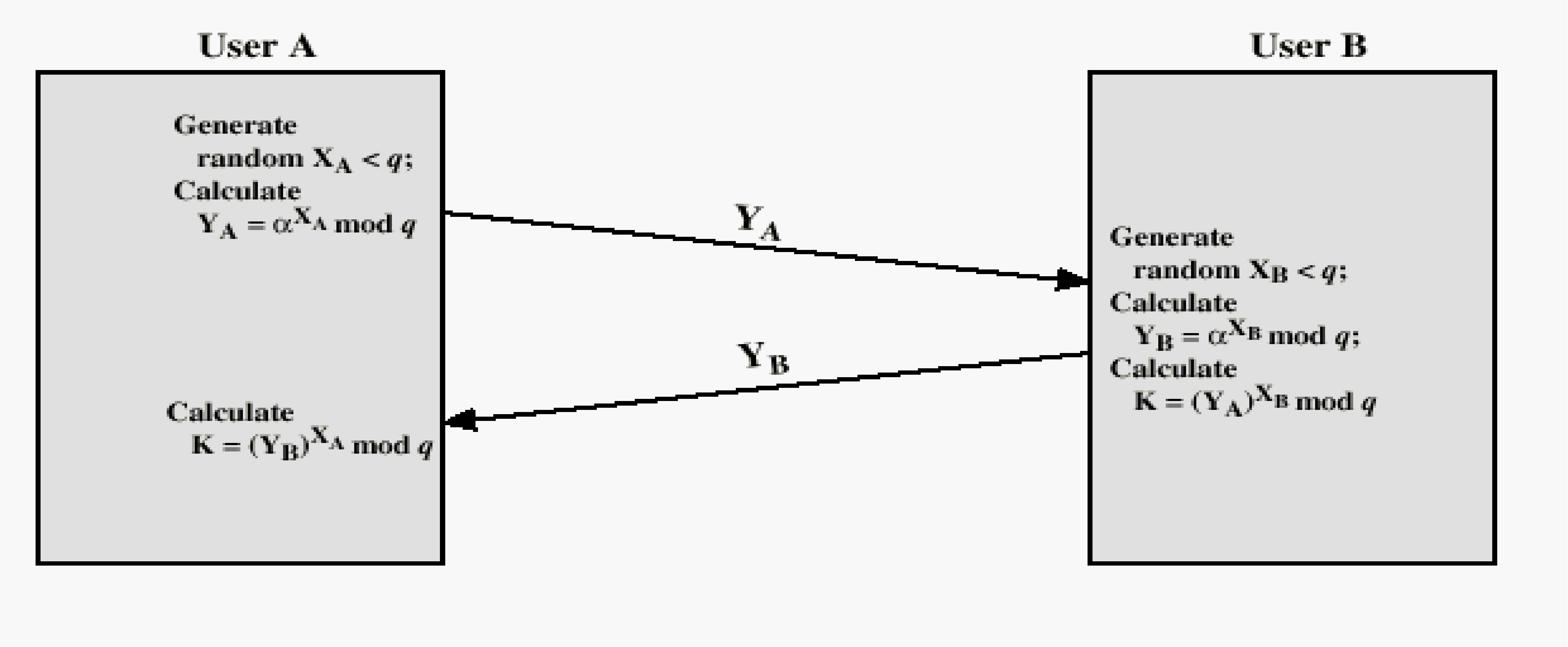
INPUT: Elliptic curve domain parameters (p, E, P, n), private key d, ciphertext (C_1, C_2)
OUTPUT: Plaintext m.

1. Compute $M = C_2 - dC_1$, and extract m from M
2. Return M.

Diffie-Hellman (DH) Key Exchange



Can you suggest ECC analog to this ?????



ECC Diffie-Hellman: ECDH

- **Public:** Elliptic curve and point B=(x,y) on curve
- **Secret:** Alice's a and Bob's b

$$\xrightarrow{a(x,y)}$$

$$\xleftarrow{b(x,y)}$$

Alice, A — Bob, B

- Alice computes a(b(x,y))
- Bob computes b(a(x,y))
- These are the same since ab = ba

Digital Signature Algorithm (DSA)

Signature Generation

INPUT: DL domain parameters (p, q, g), private key x, message m.

OUTPUT: Signature (r, s).

1. Select $k \in_R [1, q-1]$.
2. Compute $T = g^k \bmod p$
3. Compute $r = T \bmod q$. If r = 0 then go to step 1.
4. Compute h = H(m).
5. Compute $s = k^{-1}(h + xr) \bmod q$. If s = 0, then go to step 1.
6. Return (r, s).

Signature Verification

INPUT: DL domain parameters (p, q, g), public key y, message m, signature (r, s).

OUTPUT: Acceptance or Rejection of a signature.

1. Verify that r and s are integers in the interval [1, q - 1].
   If any verification fails, then return("Reject the signature").
2. Compute $h = H(m)$.
3. Compute $w = s^{-1} \bmod q$.
4. Compute $u_1 = hw \bmod q$ and $u_2 = rw \bmod q$.
5. Compute $T = g^{u1} y^{u2} \bmod p$
6. Compute $r' = T \bmod q$
7. If r = r' then return ("accept signature");
   else return("reject signature").

ECC analogue to DSA : ECDSA

Signature Generation

INPUT: Domain parameters D, private key d, message m

OUTPUT: Signature (r, s).

1. Select $k \in_R [1, n-1]$
2. Compute $kP = (x_1, y_1)$ and convert x_1 to an integer $\overline{x_1}$
3. Compute $r = \overline{x_1} \bmod n$. If r = 0 then go to step 1.
4. Compute $e = H(m)$.
5. Compute $s = k^{-1}(e + dr) \bmod n$. If s = 0 then goto step 1.
6. Return (r, s).

Signature Verification

INPUT: Domain parameters D, public key Q, message m and Signature (r, s).

OUTPUT: Acceptance or rejection of the signature

1. Verify that r and s are integers in the interval [1, n - 1].
   If any verification fails then return ("Reject the signature").
2. Compute e = H(m).
3. Compute $w = s^{-1} \bmod n$
4. Compute $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$
5. Compute $X = u_1P + u_2Q$.
6. If $X = \infty$ then return("reject signature").
7. Convert the x - coordinate x_1 to an integer $\overline{x_1}$; compute $v = \overline{x_1} \bmod n$.
8. If v = r then return("Accept the signature");
   else return("Reject the signature");

Why use ECC?

- Criteria to be considered while selecting PKC for application
  - Functionality: Does the public-key family provide the desired capabilities?
  - Security: What assurances are available that the protocols are secure?
  - Performance: For the desired level of security, do the protocols meet performance objectives?
  - Also some misc. factors such as existence of best-practice standards developed by accredited standards organizations, the availability of commercial cryptographic products, and patent coverage.

Why use ECC? (cont.)

- The RSA, DL and EC families all provide the basic functionality expected of public-key cryptography
- But…… How do we analyze these Cryptosystems?
  - How difficult is the underlying problem that it is based upon
    - RSA – Integer Factorization
    - DH – Discrete Logarithms
    - ECC - Elliptic Curve Discrete Logarithm problem

Why use ECC? (cont.)

- How do we measure difficulty?
  - We examine the algorithms used to solve these problems
  - Integer factorization
    - Number Field Sieve (NFS) : Sub exponential running time
  - Discrete Logarithm
    - Number Field Sieve (NFS) : Sub exponential running time
    - Pollard's rho algorithm
  - Elliptic Curve Discrete Logarithm (ECDL)
    - Pollard's rho algorithm : Fully exponential running time

Why use ECC? (cont.)

- To **protect** a 128 bit AES key it would take a:
  - RSA Key Size: 3072 bits
  - ECC Key Size: 256 bits
- How do we strengthen RSA?
  - Increase the key length
- **Impractical?**

NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

Applications of ECC

- Many devices are small and have limited storage and computational power
- Where can we apply ECC?
  - **Wireless communication devices**
  - Smart cards
  - Web servers that need to handle many encryption sessions
  - **Any application where security is needed but lacks the power, storage and computational power that is necessary for our current cryptosystems**

TUTORIAL QUESTIONS

Elliptic curve over real numbers

1. Does the elliptic curve equation $y^2 = x^3 - 7x - 6$ over real numbers define a group?
2. What is the additive identity of regular integers?
3. Is (4,7) a point on the elliptic curve $y^2 = x^3 - 5x + 5$ over real numbers?
4. What are the negatives of the following elliptic curve points over real numbers? P(-4,-6), Q(17,0), R(3,9), S(0,-4)
5. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is P + Q if P = (0,-4) and Q = (1,0)?
6. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is 2P if P = (4, 3.464)?

Elliptic curve over real numbers

1. Does the elliptic curve equation $y^2 = x^3 - 7x - 6$ over real numbers define a group? Ans: Yes
2. What is the additive identity of regular integers? Ans: 0
3. Is (4,7) a point on the elliptic curve $y^2 = x^3 - 5x + 5$ over real numbers? Ans: Yes
4. What are the negatives of the following elliptic curve points over real numbers? P(-4,-6), Q(17,0), R(3,9), S(0,-4) Ans: -P(-4,6), -Q(17,0), -R(3,-9), -S(0,4)
5. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is P + Q if P = (0,-4) and Q = (1,0)? Ans: P + Q = (15, -56)
6. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is 2P if P = (4, 3.464)? Ans: 2P = (12.022, -39.362)

Elliptic curve over real numbers

Consider the curve $y^2 = x^3 + 5x - 7$

Answer the following for the above curve :

1. Does the curve form group ?
2. Consider the point P(1.1, 0) on curve. Find the points 2P, 3P, 4P, 5P, 6P and 7P on curve.

Elliptic curve over real numbers

Consider the curve $y^2 = x^3 + 3x + 5$

Consider the point P(2, 2.65) on curve. Find the point 2P.

key references

- Elliptic Curves: Number Theory and Cryptography, by Lawrence C. Washington
- Guide to Elliptic Curve Cryptography, Alfred J. Menezes
- Guide to Elliptic Curve Cryptography, Darrel R. Hankerson, A. Menezes and A. Vanstone
- www.certicom.com